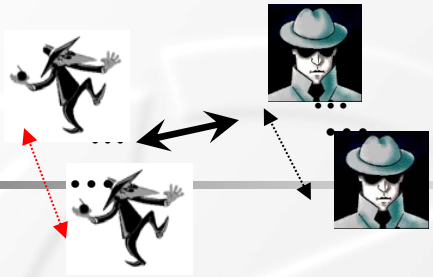


Моделирование атак, анализ защищенности и визуализация в SIEM-системах

И.В. Котенко

Санкт-Петербургский институт информатики и автоматизации РАН
(СПИИРАН)

РусКрипто'2013, 27-30 марта 2013 г.

План доклада

- Введение
- SIEM-системы
- Проект MASSIF
- Аналитическое моделирование
- Анализ защищенности
- Визуализация
- Заключение

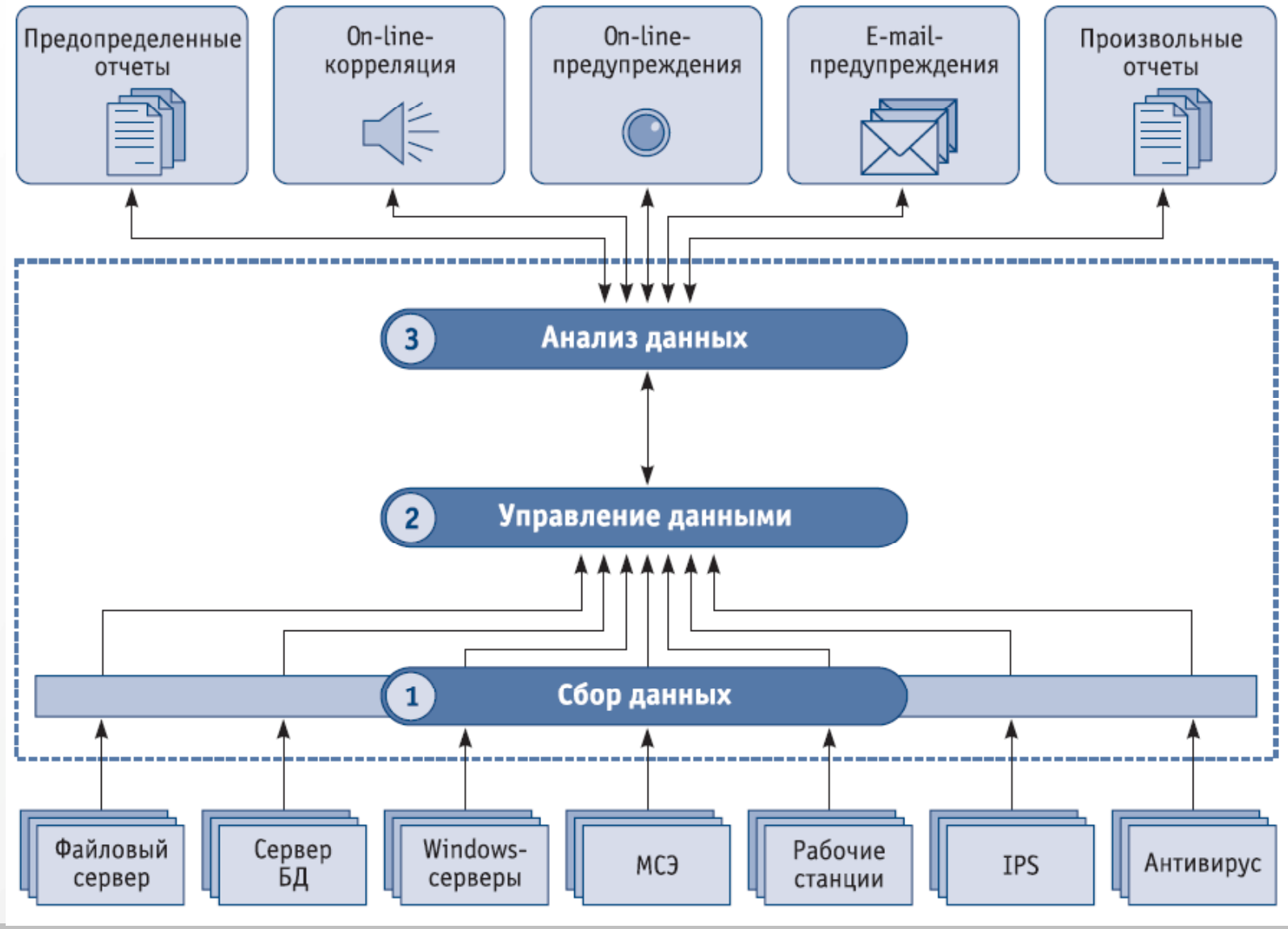
Понятие SIEM-системы

Security information and event management (SIEM) system – система управления информацией и событиями безопасности.

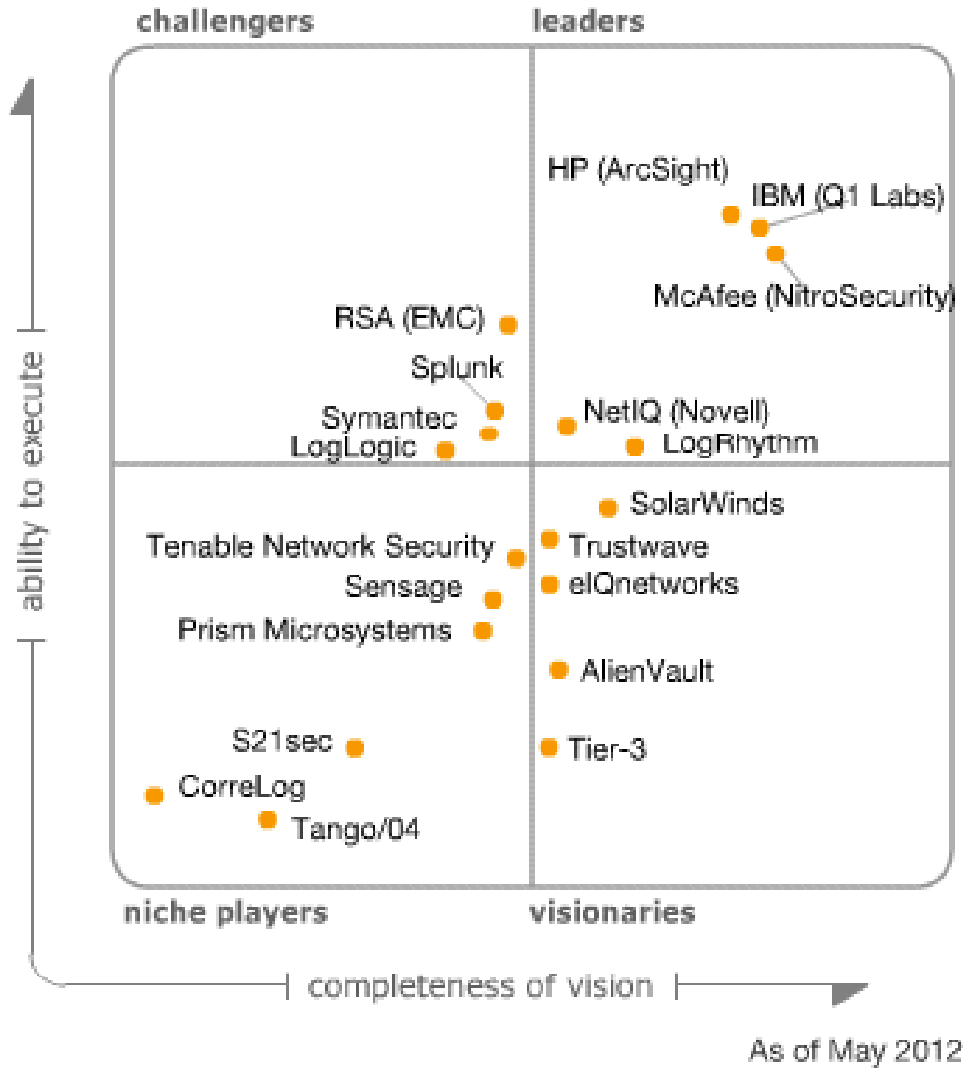
Технология SIEM = SIM + SEM

Основная цель SIEM – повышение ИБ за счет обеспечения возможности в режиме, близком к реальному времени, манипулировать ***информацией о безопасности*** и осуществлять проактивное ***управление инцидентами и событиями безопасности***

Архитектура типовой SIEM-системы

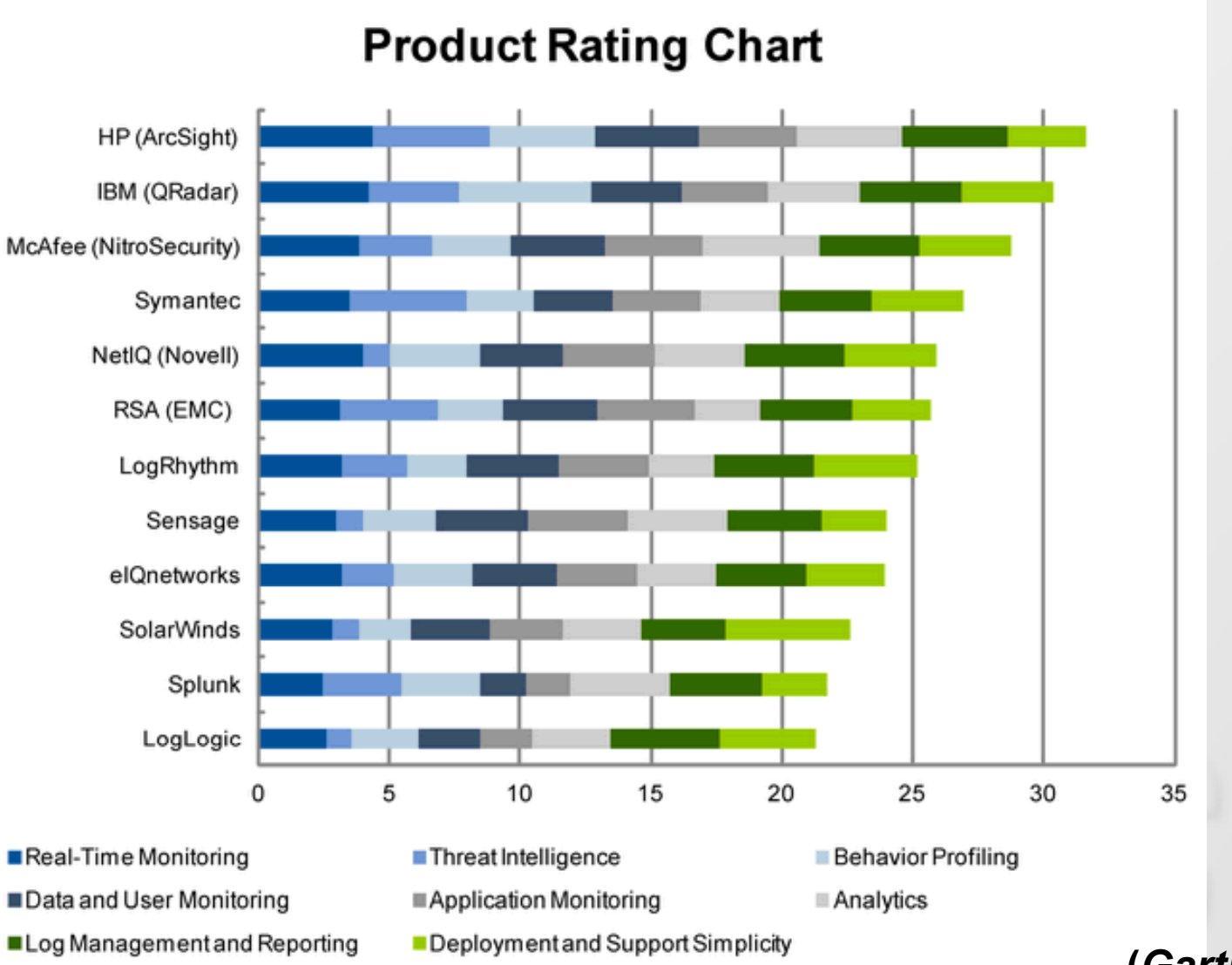


Сравнение SIEM-решений (1/2)



(*Gartner, 2012*)

Сравнение SIEM-решений (2/2)



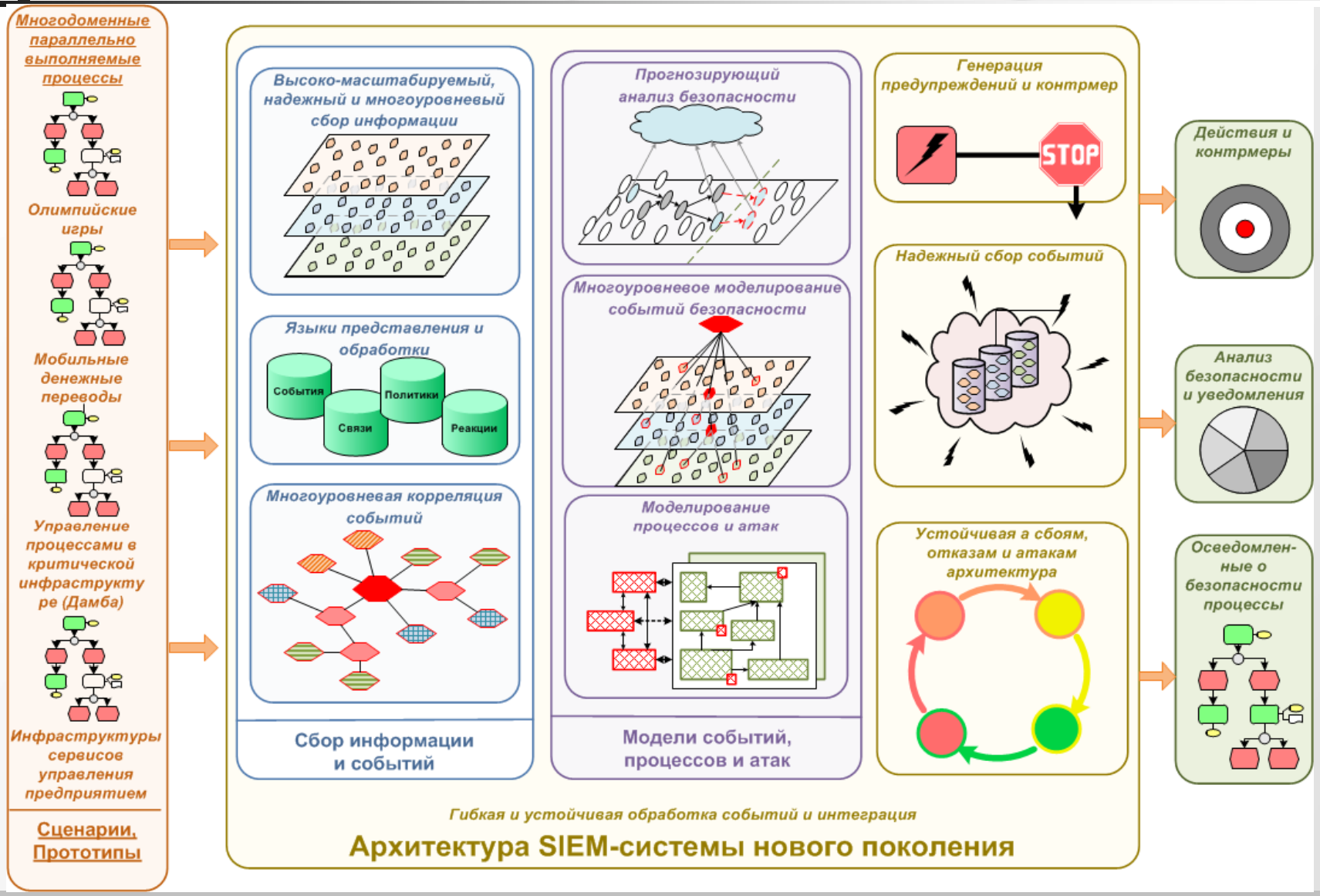
(*Gartner, 2012*)

План доклада

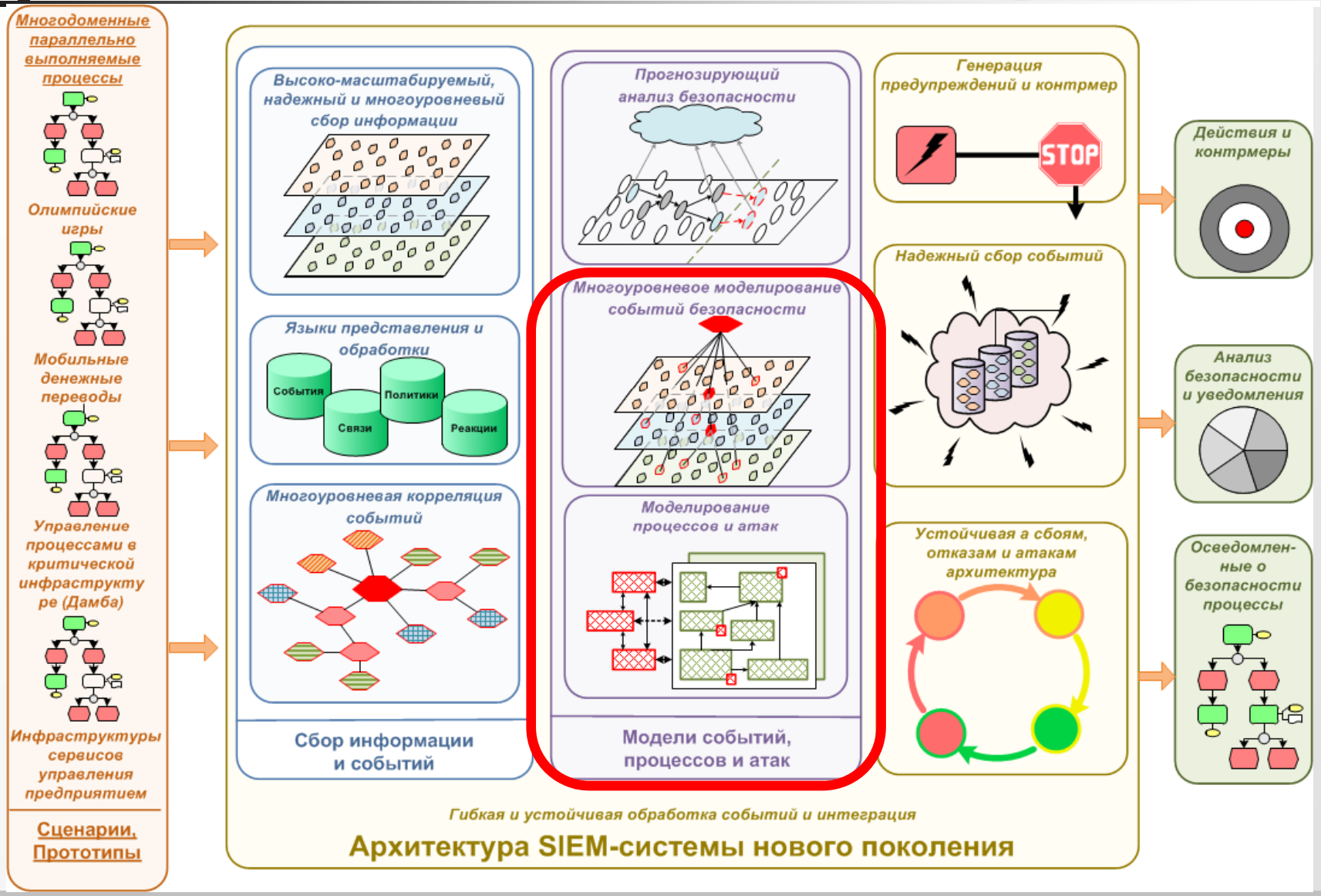
- Введение
- SIEM-системы
- **Проект MASSIF**
- Аналитическое моделирование
- Анализ защищенности
- Визуализация
- Заключение

SPIRAS

Цели, задачи и структура проекта Евросоюза MASSIF



Место и роль исследуемых процессов в проекте MASSIF (1/2)



План доклада

- Введение
- SIEM-системы
- Проект MASSIF
- **Аналитическое моделирование**
- Анализ защищенности
- Визуализация
- Заключение

Базовые работы по моделированию атак для анализа механизмов защиты (1/2)

- Проверка на модели (C.Ramakrishnan и R.Sekar, R.Ritchey и P.Ammann, O.Sheyner, S.Jha и J.Wing – SMV, NuSMV, SPIN). Требуют определить гипотезу (состояние системы), нарушение которой проверяется методом model checking
- Экспертные системы (M.Danforth – Java Expert System Shell). Правила – выполнение атакующих действий, факты – состояния системы. Атаки в виде предусловия/постусловия
- Логический подход (X.Ou, W.Boyer, M.McQueen – Datalog language). Граф состоит из вершин вывода и вершин фактов. Модель сети – множество высказываний Datalog, атаки – правила Datalog
- Графы атак. Например C.Philips и L.Swiler строят граф: вершины – состояния системы, дуги – переходы [Ortalo et al., 1999; Ritchey&Ammann, 2000; Sheyner et al., 2002; Rieke, 2004; Noel&Jajodia, 2005; Lippmann&Ingols, 2006; …]

Базовые работы по моделированию атак для анализа механизмов защиты (2/2)

- Представление сценариев атак и моделей нарушителей [Schneier, 1999; Dawkins et al., 2002; Shepard et al., 2005; …]
- Спецификация платформ, уязвимостей, оценок уязвимостей, атак, слабостей и конфигураций [NVD; OSVDB; CVE; CVSS; CPE; CCE; CWE; CAPEC; …]
- Показатели защищенности [Mell et al., 2007; Jaquith, 2007; Herrmann, 2007; Jansen, 2009; …]
- Комбинирование графов зависимостей сервисов и графов атак [Kheir et al., 2009; Kheir et al., 2010; …]
- Представление атак нулевого дня [Ingols et al., 2009; Wang et al., 2010; …]
- Моделирование контрмер [Kheir et al., 2010; …]

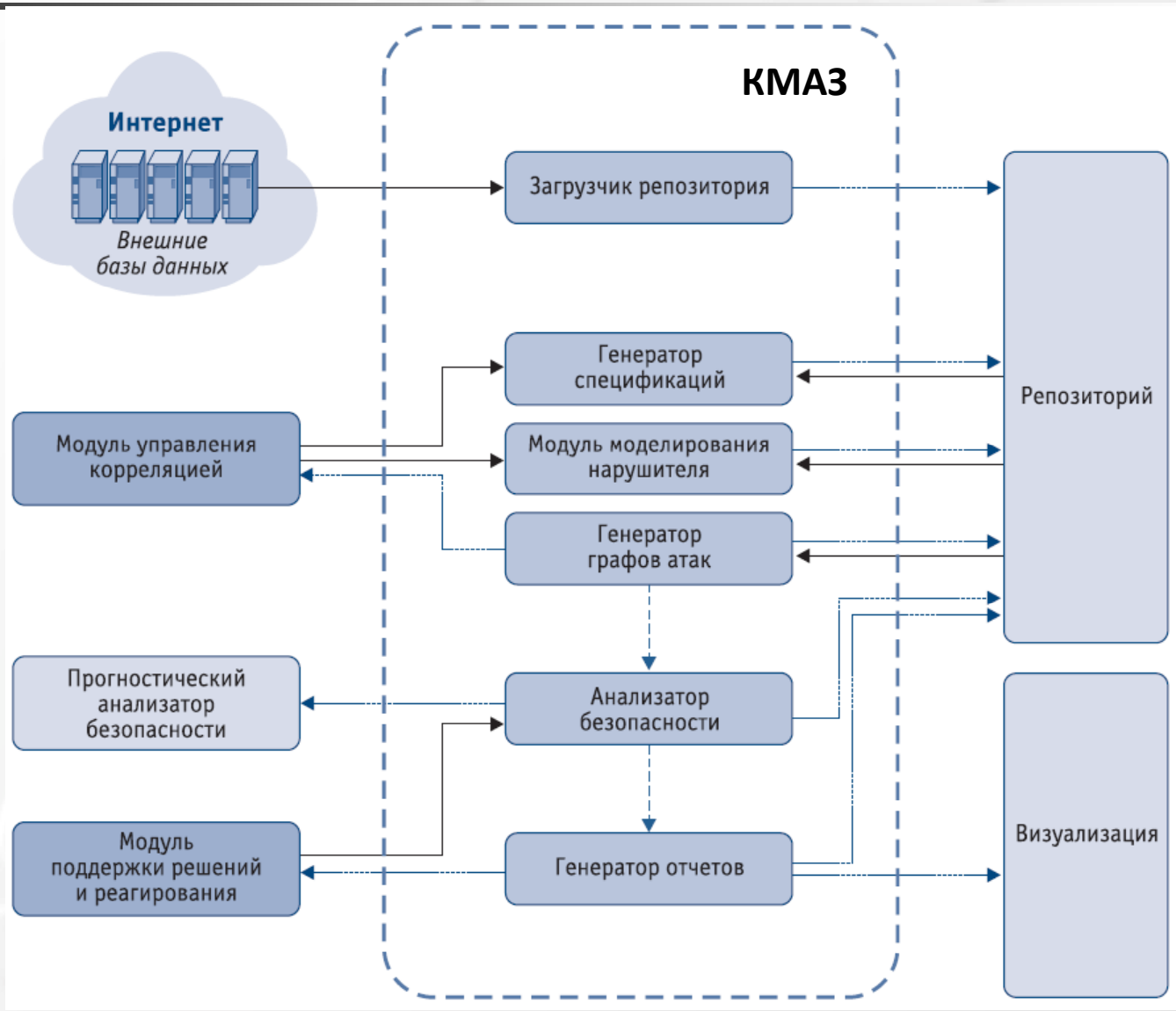
Особенности предлагаемых решений (1/2)

- Использование репозитория безопасности (содержащего данные о конфигурации системы, моделях нарушителя, уязвимостях, атаках, оценках, контрмерах и др.)
- Эффективные методики генерации графов атак и зависимостей сервисов, базирующиеся на методиках топологического анализа уязвимостей (TVA), которые формируют потенциальные последовательности использования уязвимостей для построения графов атак
- Учет как известных, так и новых атак, основанных на уязвимостях 0-го дня
- Применение anytime-алгоритмов для обеспечения близкого к реальному времени генерации подграфов атак и процедур анализа защищенности (anytime-алгоритм - итерационный вычислительный алгоритм, который способен выдать наилучшее на данный момент решение)

Особенности предлагаемых решений (2/2)

- Комбинированное использование графов атак и графов зависимостей сервисов
- Вычисление комплекса разнообразных показателей защищенности, включая следующие показатели:
  - уровень защищенности,
  - уровень воздействия и потенциал атаки,
  - уровень навыков нарушителя,
  - эффективность контрмер,
  - степень побочных потерь при реализации контрмер и др.
- Стохастическое аналитическое моделирование и интерактивная поддержка принятия решений для выбора предпочтительных решений по безопасности на основе определения предпочтений относительно различных типов целей и требований (рисков, стоимости, выигрыша) и установления компромиссов между высокоуровневыми целями защиты информации

Архитектура компонента аналитического моделирования

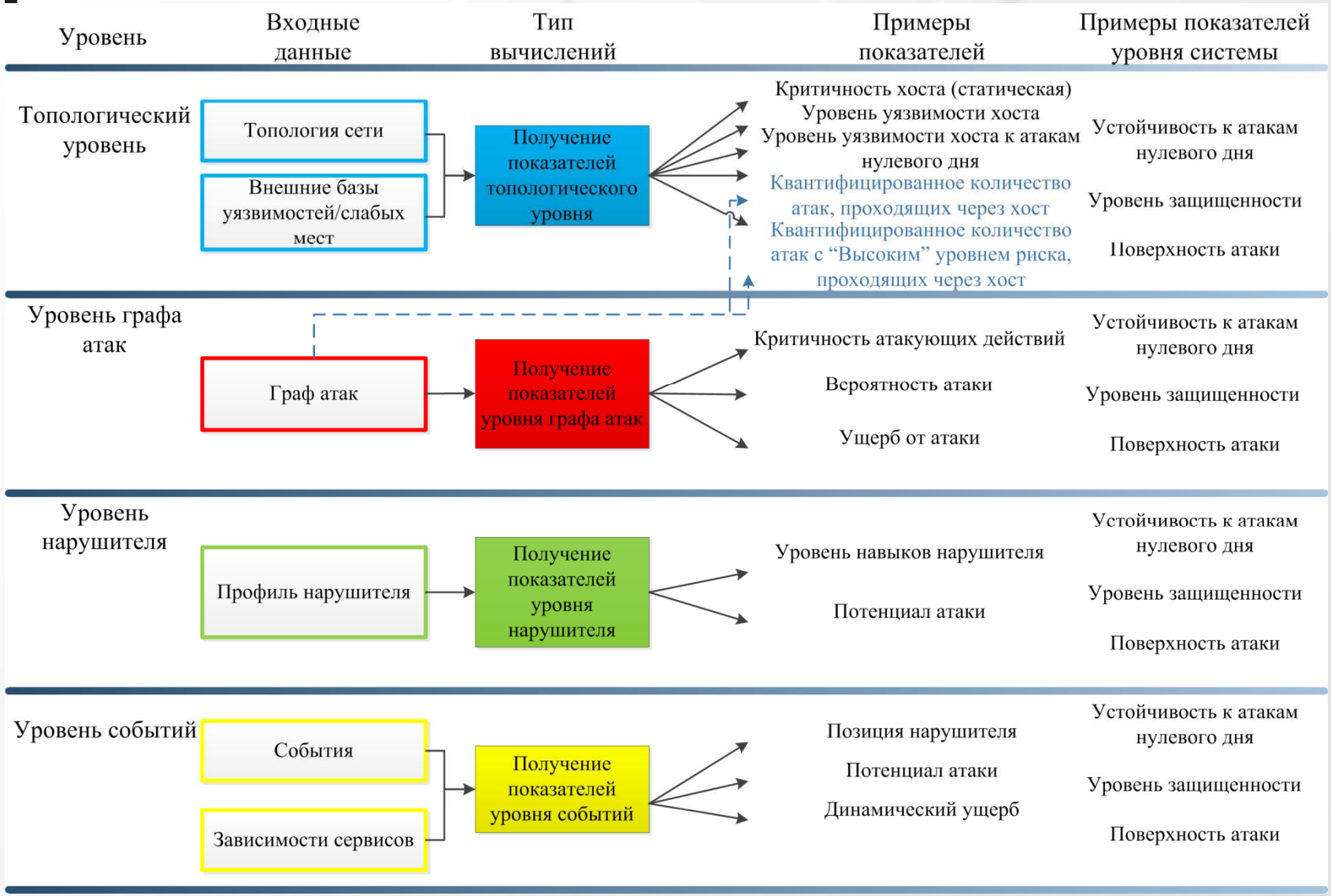


План доклада

- Введение
- SIEM-системы
- Проект MASSIF
- Аналитическое моделирование
- **Анализ защищенности**
- Визуализация
- Заключение

SPIRAS

Показатели защищенности и уровни оценки



Методики вычисления показателей защищенности

1. **Статическая методика экспресс оценки уровня защищенности**

   Методика, определяющая общий уровень защищенности системы на основе учета возможности реализации угроз и их последствий для системы.

2. **Методика, учитывающая события безопасности, происходящие в системе**

   Ориентирована на работу в реальном времени, когда текущее положение атакующего и его перемещение в сети может отслеживаться, но существуют жесткие ограничения на время вычислений.

3. **Методика, основанная на анализе исторических данных**

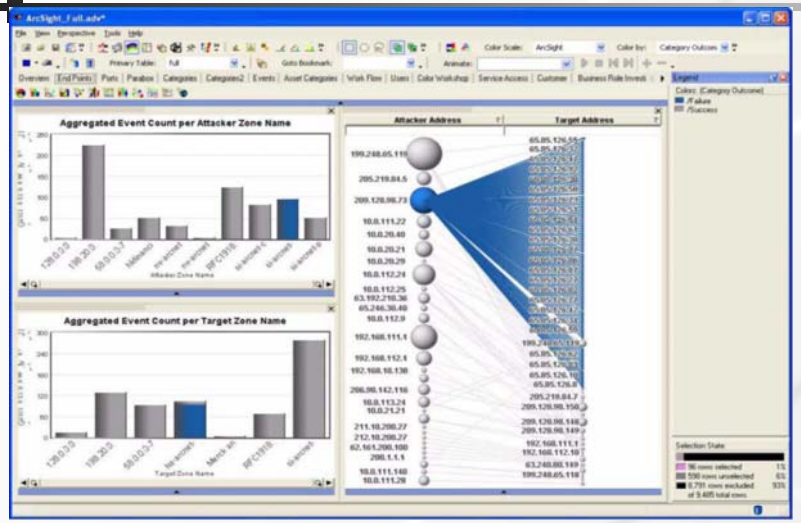
   При вычислении вероятности и потенциала атаки используются данные о предыдущих инцидентах.

План доклада

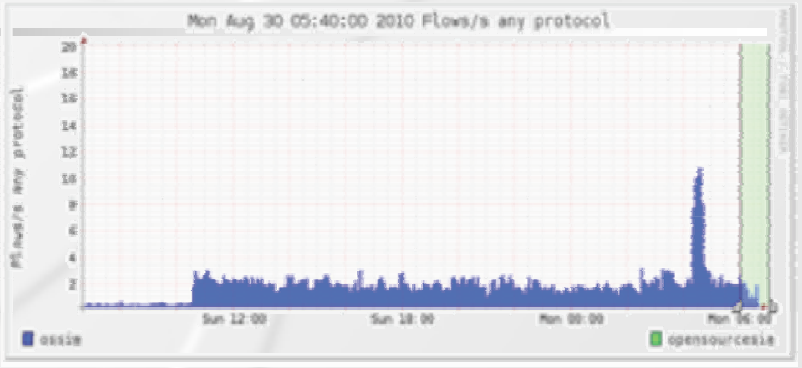
- Введение
- SIEM-системы
- Проект MASSIF
- Аналитическое моделирование
- Анализ защищенности
- **Визуализация**
- Заключение

SPIRAS

Модели визуализации в SIEM-системах

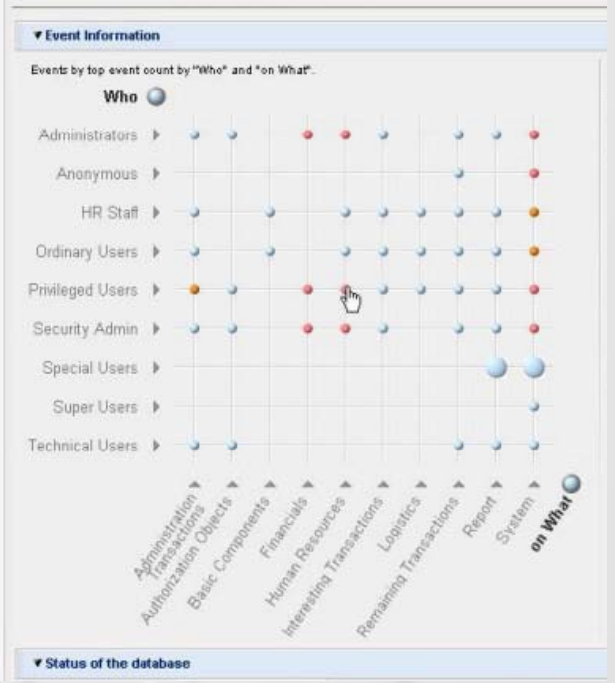


Arcsight: обнаружение атак



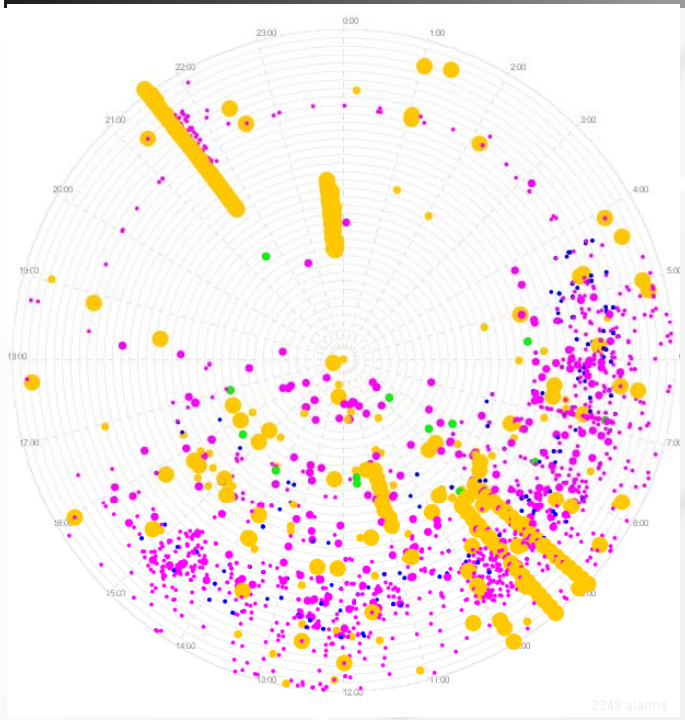
OSSIM: визуализация сетевого трафика

OSSIM: отчет об уязвимостях

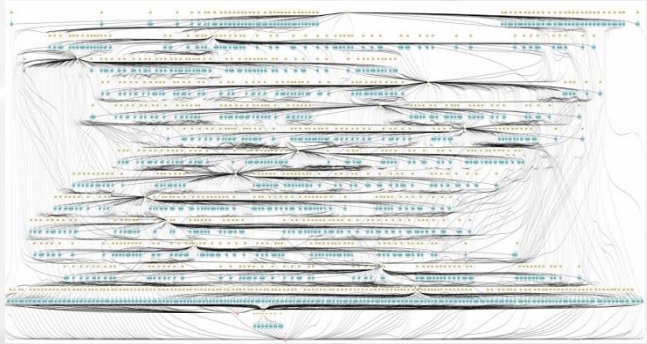


TSIEM: представление правил доступа

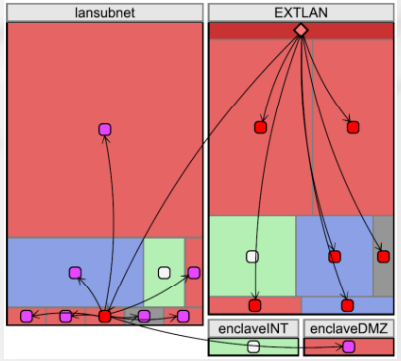
Модели визуализации для представления событий и анализа защищенности

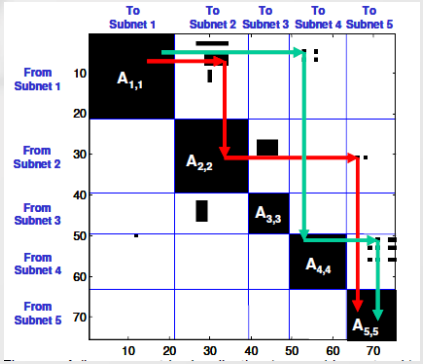


Представление событий в SpiralView [1]



Визуализация атак на основе графов [2]





Альтернативные представления атак [3, 4]

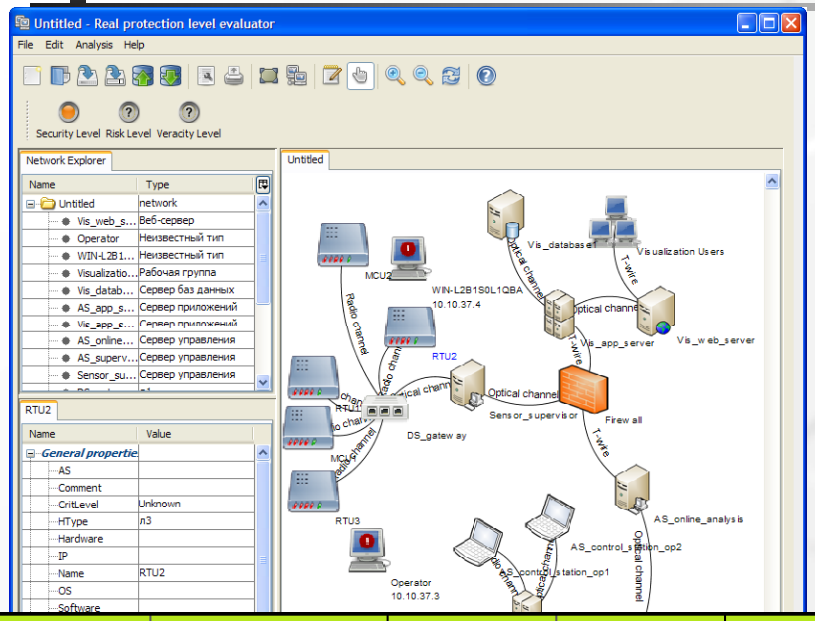
[1] Bertini E., Hertzog P., Lalanne D. SpiralView: Towards Security Policies Assessment through Visual Correlation of Network Resources with Evolution of Alarms. In Proceedings of the IEEE Symposium on Visual Analytics Science and Technology (VAST) 2007. pp.139-146.

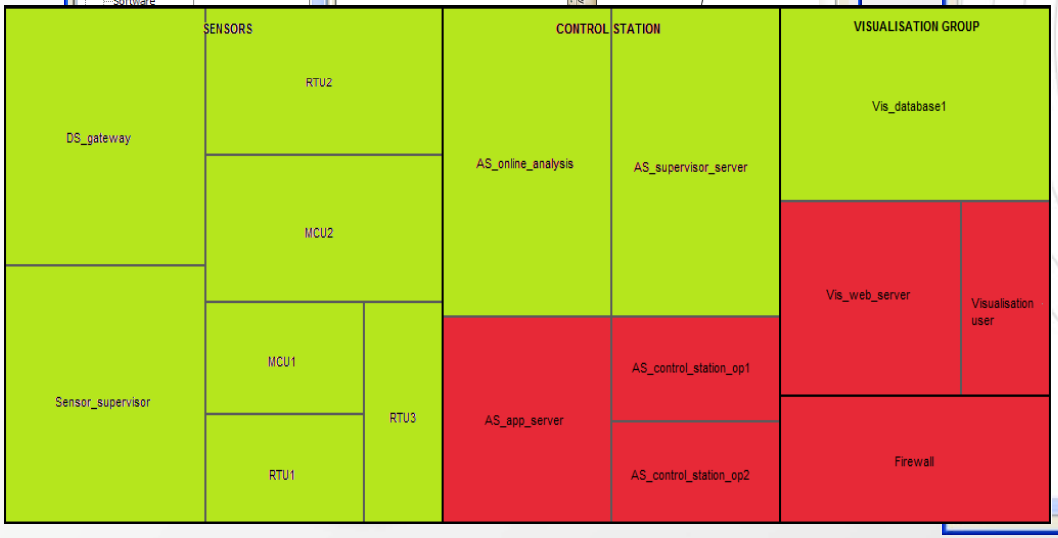
[2] Noel S.. Managing attack graph complexity through visual hierarchical aggregation. In Proceedings of ACM workshop on Visualization and data mining for computer security (VizSEC/DMSEC '04), NY., ACM press, 2004, pp.109-118.

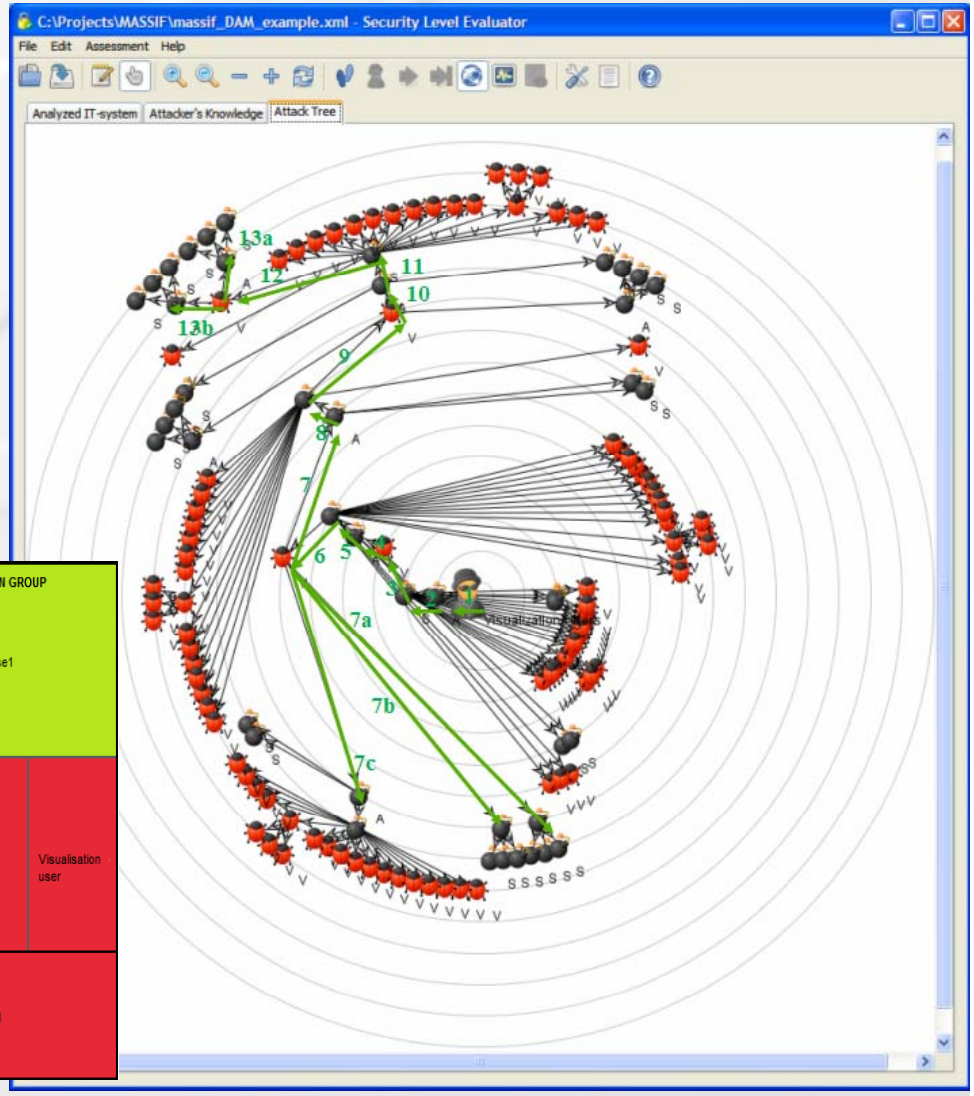
[3] Williams L., Lippmann R., Ingols K. An Interactive Attack Graph Cascade and Reachability Display. In Proceedings of the Workshop on Visualization for Computer Security, Sacramento, California, USA, 2008. Springer, Heidelberg. pp. 221-236.

[4] Noel S., Jajodia S. Understanding complex network attack graphs through clustered adjacency matrices. In Proceedings of the 21st Annual Computer Security Applications Conference, 2005, pp.160-169.

Примеры интерфейсов компонента моделирования и анализа защищенности







Главное окно (1/2)

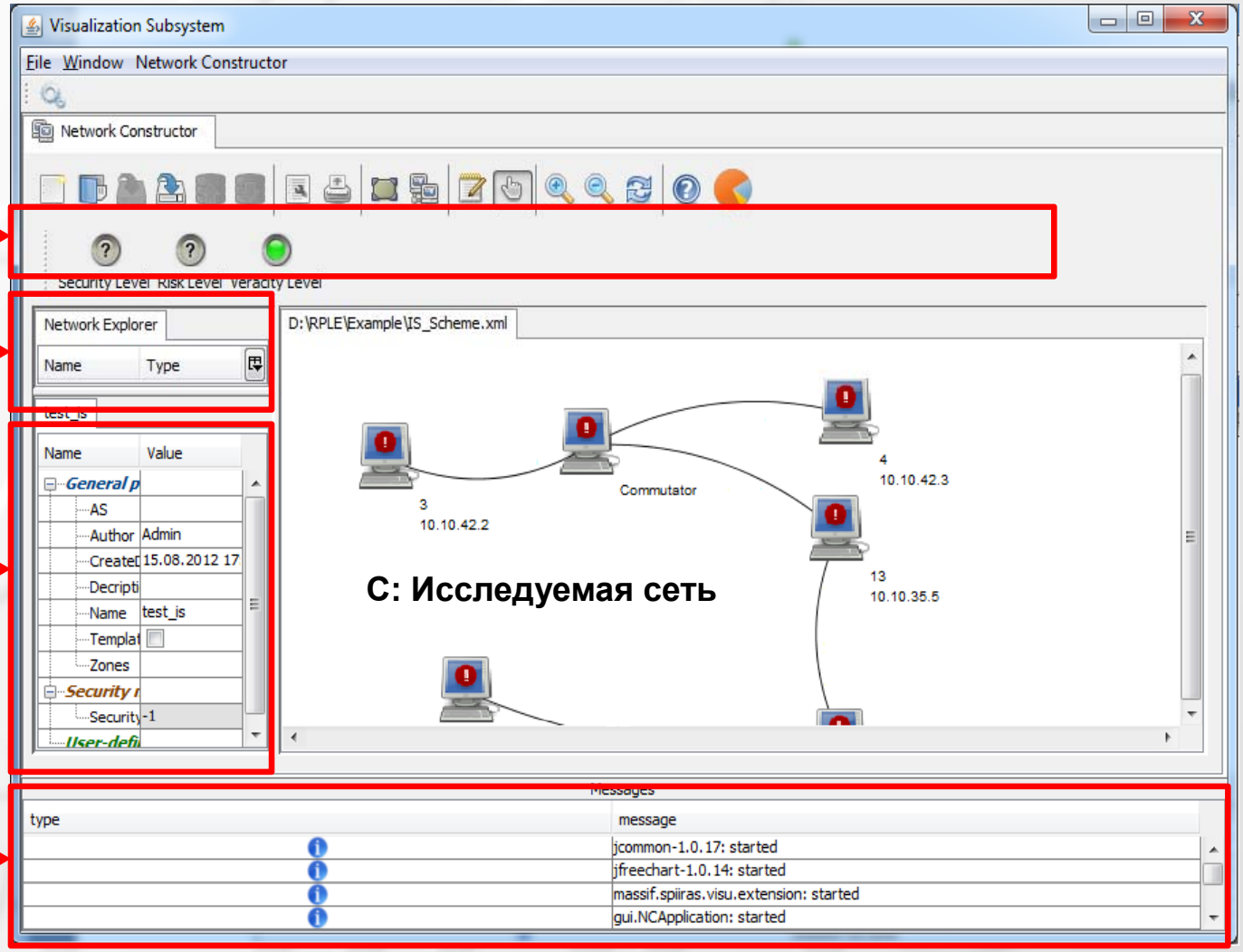
При спецификации сети

D: Network security metrics
Для быстрого доступа

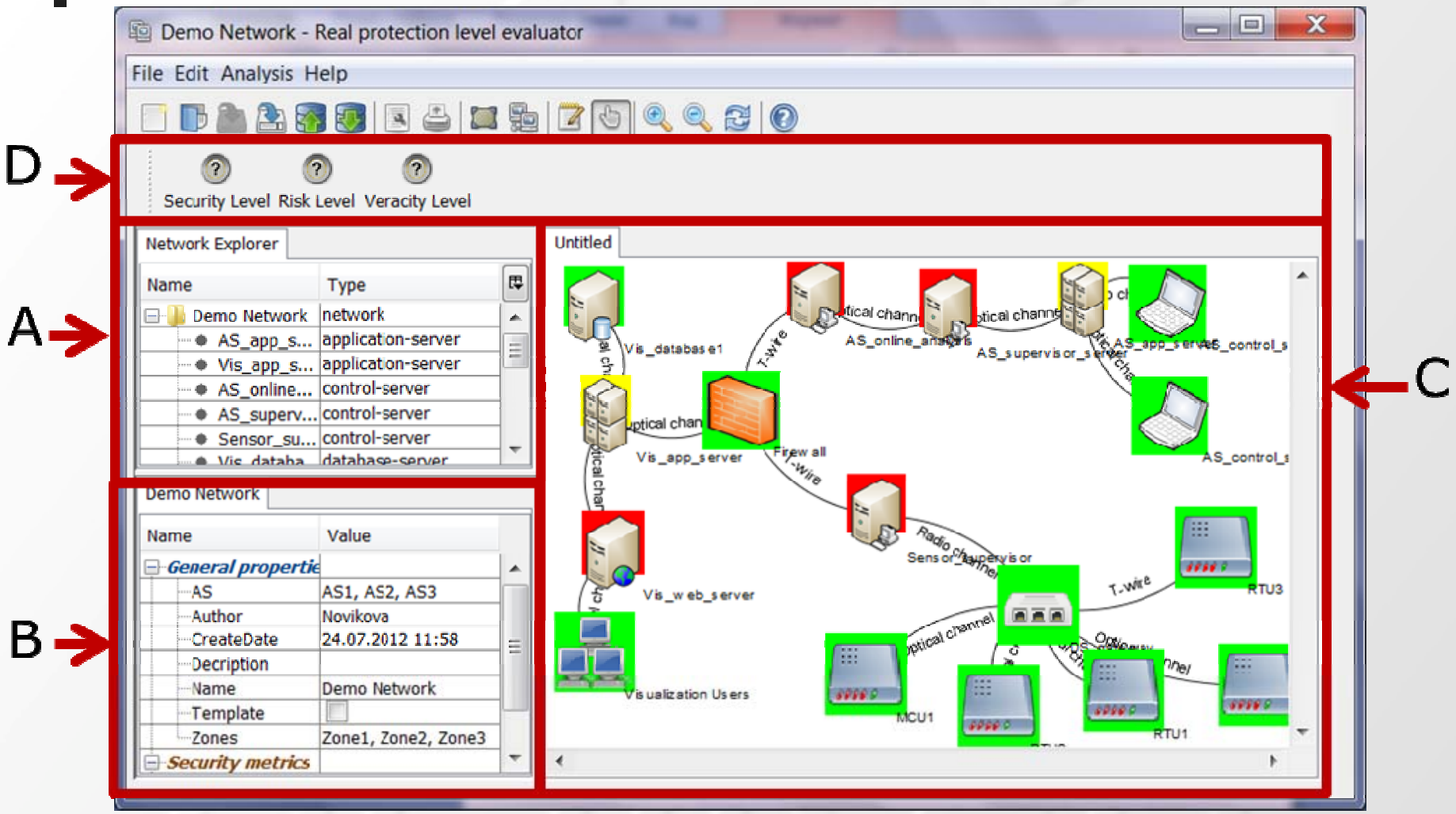
A: Network Explorer
Для быстрого просмотра сети

B: Property explorer
Для конфигурирования узлов сети

System messages



Главное окно (2/2)



План доклада

- Введение
- SIEM-системы
- Проект MASSIF
- Аналитическое моделирование
- Анализ защищенности
- Визуализация
- **Заключение**

SPIRAS

Основные результаты работы

- Представлен подход к моделированию атак и механизмов защиты, анализу защищенности и визуализации в SIEM-системах.
- Разработаны средства аналитического моделирования, анализа защищенности и визуализации, реализующие данный подход.
- Предлагаемый подход к моделированию позволяет исследовать различные механизмы построения защищенных сетей, отвечать на вопросы “Что, если…”, определять наиболее эффективные механизмы защиты, осуществлять анализ защищенности в режиме, близком к реальному времени.

Направления дальнейших исследований

- Совершенствование моделей базовых компонентов и их реализация
- Улучшение масштабируемости и адекватности аналитического моделирования
- Разработка подхода и стенда моделирования, основанных на “многорезолюционных” методах моделирования. Данный подход позволяет интегрировать макро- и микро- уровневые модели атак и механизмов защиты *(аналитические, основанные на пакетах, базирующиеся на эмуляции) и реальные сети небольшого размера для исследования масштабных атак и механизмов защиты.*

Контактная информация

Котенко Игорь Витальевич (СПИИРАН)
ivkote@comsec.spb.ru
http://comsec.spb.ru/kotenko/

Благодарности

- Работа выполняется при финансовой поддержке РФФИ, программы фундаментальных исследований ОНИТ РАН (проект № 2.2), государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

РОССИЙСКАЯ АКАДЕМИЯ НАУК